

ELECTRONIC CHECK SYSTEM

Patent Number: JP9218905
Publication date: 1997-08-19
Inventor(s): YOSHIDA AKIO; IEGI TOSHIATSU; ICHIHARA NAOHISA
Applicant(s): N T T DATA TSUSHIN KK
Requested Patent: ☐ JP9218905
Application Number: JP19960022380 19960208
Priority Number(s):
IPC Classification: G06F19/00; G07F7/08
EC Classification:
Equivalents: JP3365599B2

Abstract

PROBLEM TO BE SOLVED: To detect the copy use of an electronic check by communication between interested parties and to make a payment by a received electronic check.

SOLUTION: The secret key and public key of each user and the public key of a bank are stored in an IC card possessed by the user. When the user 11 sends the electronic check to the other user 27, the respective public keys are mutually informed between the IC cards 45 and 47 and a random number is informed from the IC card 47 of a receiver 27 to the IC card 45 of a payer 11. The IC card 45 on a paying side changes the sequence of a progression included in the electronic check based on the random number, ciphers it by the public key of the receiver 27 and transmits it to the IC card 47 on a receiving side. The IC card 47 on the receiving side deciphers the electronic check by the secret key of the receiver 27, confirms the propriety of a bank signature by the public key of the bank, confirms whether or not the sequence of the progression is correctly changed corresponding to the random number and formally receives the electronic check.

Data supplied from the esp@cenet database - I2

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-218905

(43) 公開日 平成9年(1997)8月19日

(51) Int.Cl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 19/00			G 0 6 F 15/30	3 6 0
G 0 7 F 7/08				3 5 0
			G 0 7 F 7/08	R

審査請求 未請求 請求項の数11 O L (全 21 頁)

(21) 出願番号 特願平8-22380

(22) 出願日 平成8年(1996)2月8日

(71) 出願人 000102728

エヌ・ティ・ティ・データ通信株式会社
東京都江東区豊洲三丁目3番3号

(72) 発明者 吉田 明雄

東京都江東区豊洲三丁目3番3号 エヌ・
ティ・ティ・データ通信株式会社内

(72) 発明者 家木 俊温

東京都江東区豊洲三丁目3番3号 エヌ・
ティ・ティ・データ通信株式会社内

(72) 発明者 市原 尚久

東京都江東区豊洲三丁目3番3号 エヌ・
ティ・ティ・データ通信株式会社内

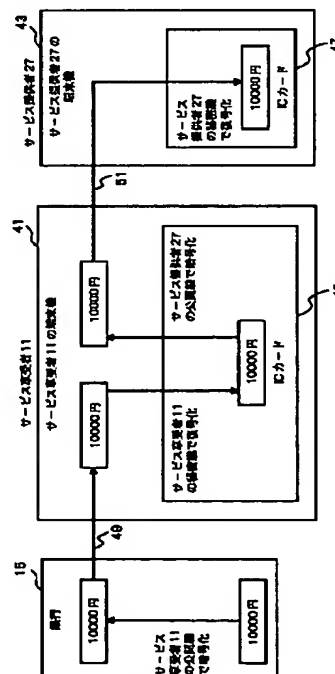
(74) 代理人 弁理士 上村 輝之

(54) 【発明の名称】 電子小切手システム

(57) 【要約】 (修正有)

【課題】 当事者間の通信で電子小切手のコピー使用の検出ができ、受領した電子小切手で支払いが行える。

【解決手段】 利用者が所持する IC カードには、各々の利用者の秘密鍵、公開鍵及び銀行の公開鍵が記憶され、利用者 11 が他の利用者 27 へ電子小切手を送る場合は、IC カード 45、47 間で各々の公開鍵が相互通知されると共に、受領者 27 の IC カード 47 から支払者 11 の IC カード 45 へ乱数が通知される。支払側 IC カード 45 は、電子小切手に含まれている数列の順序を、乱数に基づいて変更した上で、受領者 27 の公開鍵で暗号化して受領側 IC カード 47 へ送信する。受領側 IC カード 47 は、その電子小切手を受領者 27 の秘密鍵で復号化し、銀行署名の正当性を銀行の公開鍵で確認し、数列の順序が乱数に従って正しく変更されているかを確認して、電子小切手を正式に受領する。



【特許請求の範囲】

【請求項1】 電子商取引に適用される電子小切手システムにおいて、
電子小切手の振出し及び決済を行う銀行のコンピュータと、前記電子小切手を利用する複数の利用者の各々が所持するICカードとを備え、
前記銀行コンピュータが、振出した電子小切手に前記銀行の電子署名を含ませる署名手段を有し、
前記各利用者のICカードが、
前記各利用者の秘密鍵を、ICカード外部への読み出しが不可能な状態で記憶する秘密鍵記憶手段と、
前記各利用者の公開鍵及び前記銀行の公開鍵を記憶する公開鍵記憶手段と、
前記銀行コンピュータ及び他の利用者のICカードのいずれかである支払者装置から電子小切手を受信するとき、前記支払者装置へ前記各利用者の公開鍵を送信する公開鍵送信手段と、
前記支払者装置から前記電子小切手を受信する小切手受信手段と、
前記受信した電子小切手を前記各利用者の秘密鍵を用いて復号化する小切手復号化手段と、
前記復号化した電子小切手に含まれている前記銀行の署名が正しいことを、前記銀行の公開鍵を用いて確認する署名確認手段と、
前記銀行署名が正しいことが確認されたとき、前記受信した電子小切手を受領したものとして記憶する小切手記憶手段と、
前記小切手記憶手段内の電子小切手を前記他の利用者のICカードへ送信するとき、前記他の利用者のICカードから前記他の利用者の公開鍵を受信する公開鍵受信手段と、
前記小切手記憶手段内の電子小切手を、前記受信した他の利用者の公開鍵によって暗号化する小切手暗号化手段と、
前記暗号化した電子小切手を、前記他の利用者のICカードへ送信する小切手送信手段とを有することを特徴とする電子小切手システム。

【請求項2】 請求項1記載の電子小切手システムにおいて、
前記各利用者のICカードが、前記利用者の秘密鍵と公開鍵とを生成する鍵生成手段をさらに有することを特徴とする電子小切手システム。

【請求項3】 請求項2記載の電子小切手システムにおいて、
前記銀行コンピュータが、前記ICカードを利用者に発行する手段をさらに有し、
前記ICカードの鍵生成手段が、発行されたときに前記利用者の秘密鍵と公開鍵とを生成して、生成した利用者の公開鍵を前記銀行のコンピュータに通知することを特徴とする電子小切手システム。

【請求項4】 請求項1、2及び3のいずれか一項に記載の電子小切手システムにおいて、
前記銀行コンピュータが、前記振出した電子小切手に、一定の順序で並んだ複数の数字を含ませる数字列付加手段をさらに有し、
前記各利用者のICカードが、
前記他の利用者のICカードから前記電子小切手を受信するとき、第1の乱数を発生させて前記他の利用者のICカードに送信する乱数発生手段と、
前記受信した電子小切手に含まれている前記複数の数字の順序が、前記通知した第1の乱数に従って一定の規則の下で正しく変更されていることを確認する数字順序確認手段と、
前記小切手記憶手段内の電子小切手を、前記銀行コンピュータ及び他の利用者のICカードのいずれかである受領者装置へ送信するとき、前記受領者装置が発生させた第2の乱数を前記受領者装置から受信する乱数受信手段と、
前記小切手記憶手段内の電子小切手に含まれている前記複数の数字を、前記受信した第2の乱数に従って前記一定の規則の下で変更する順序変更手段とを更に有し、
前記各利用者のICカードの前記小切手記憶手段が、前記銀行署名が正しいことが確認されたのに加え、前記受信した電子小切手の数字順序が正しく変更されていることが確認されたとき、前記受信した電子小切手を受領したものとして記憶することを特徴とする電子小切手システム。

【請求項5】 請求項4記載の電子小切手システムにおいて、
前記銀行のコンピュータが、
前記銀行の秘密鍵を、銀行外部への読み出しが不可能な状態で記憶する銀行秘密鍵記憶手段と、
前記銀行の公開鍵及び利用者の公開鍵を記憶する銀行公開鍵記憶手段と、
前記振出した電子小切手を、前記利用者の公開鍵によって暗号化する振出小切手暗号化手段と、
暗号化した前記振出した電子小切手を、前記利用者のICカードの一つへ送信する振出小切手送信手段と、
前記利用者のICカードから決済対象の電子小切手を受信する決済小切手受信手段と、
前記受信した決済対象の電子小切手を前記銀行の秘密鍵を用いて復号化する決済小切手復号化手段と、
前記復号化した決済対象の電子小切手に含まれている前記銀行署名が正しいことを、前記銀行の公開鍵を用いて確認する銀行署名確認手段と、
前記決済対象の電子小切手の銀行署名が正しいことが確認されたとき、前記決済対象の電子小切手による決済を実行する決済実行手段と、
をさらに有することを特徴とする電子小切手システム。

【請求項6】 請求項5記載の電子小切手システムにお

いて、
前記銀行コンピュータが、
前記各利用者のＩＣカードから前記決済対象の電子小切手を受信するときに、
前記第２の乱数を発生させて前記ＩＣカードに通知する銀行乱数発生手段と、
前記受信した決済対象の電子小切手に含まれている前記複数の数字の順序が、前記通知した第２の乱数に従って一定の規則の下で正しく変更されていることを確認する銀行数字順序確認手段と、を更に有し、
前記銀行コンピュータの前記決済実行手段が、前記銀行署名が正しいことが確認されたのに加え、前記決済対象の電子小切手の数字順序が正しく変更されていることが確認されたとき、前記決済対象の電子小切手の決済を実行することを特徴とする電子小切手システム。

【請求項７】 電子商取引に適用される電子小切手システムにおいて、
電子小切手の振出し及び決済を行う銀行のコンピュータと、前記電子小切手を利用する複数の利用者の各々が所持するＩＣカードとを備え、
前記銀行コンピュータが、振出した電子小切手に、一定の順序で並んだ複数の数字を含ませる数字列付加手段を有し、
前記各利用者のＩＣカードが、
前記他の利用者のＩＣカードから電子小切手を受信する前に、第１の乱数を発生させて前記他の利用者のＩＣカードに送信する乱数発生手段と、
前記他の利用者のＩＣカードから前記電子小切手を受信する小切手受信手段と、
前記受信した電子小切手に含まれている前記複数の数字の順序が、前記通知した第１の乱数に従って一定の規則の下で正しく変更されていることを確認する数字順序確認手段と、
前記受信した電子小切手の数字順序が正しく変更されていることが確認されたとき、前記受信した電子小切手を受領したものとして記憶する小切手記憶手段と、
前記小切手記憶手段内の電子小切手を、前記銀行コンピュータ及び他の利用者のＩＣカードのいずれかである受領者装置へ送信する前に、前記受領者装置が発生させた第２の乱数を前記受領者装置から受信する乱数受信手段と、
前記小切手記憶手段内の電子小切手に含まれている前記複数の数字を、前記受信した第２の乱数に従って前記一定の規則の下で変更する順序変更手段と、
前記順序変更手段によって前記数字順序が変更された前記電子小切手を、前記受領者装置に送信する小切手送信手段と、を有することを特徴とする電子小切手システム。

【請求項８】 請求項７記載の電子小切手システムにおいて、

前記銀行コンピュータが、
前記各利用者のＩＣカードから決済対象の電子小切手を受信する前に、前記第２の乱数を発生させて前記ＩＣカードに通知する銀行乱数発生手段と、
前記各利用者のＩＣカードから前記決済対象の電子小切手を受信する決済小切手受信手段と、
前記受信した決済対象の電子小切手に含まれている前記複数の数字の順序が、前記通知した第２の乱数に従って一定の規則の下で正しく変更されていることを確認する銀行数字順序確認手段と、
前記決済対象の電子小切手の数字順序が正しく変更されていることが確認されたとき、前記決済対象の電子小切手の決済を実行する決済実行手段とを有することを特徴とする電子小切手システム。

【請求項９】 請求項７に記載の電子小切手システムにおいて、
前記複数の数字の各々が乱数であることを特徴とする電子小切手システム。

【請求項１０】 銀行のコンピュータから振出された電子小切手であって、前記銀行の電子署名が付与されている電子小切手を格納するために、複数の利用者の各々が所持するＩＣカードにおいて、
前記各利用者の秘密鍵を、ＩＣカード外部への読み出しが不可能な状態で記憶する秘密鍵記憶手段と、
前記各利用者の公開鍵及び前記銀行の公開鍵を記憶する公開鍵記憶手段と、
前記銀行コンピュータ及び他の利用者のＩＣカードのいずれかである支払者装置から電子小切手を受信するとき、前記支払者装置へ前記各利用者の公開鍵を送信する公開鍵送信手段と、
前記支払者装置から前記電子小切手を受信する小切手受信手段と、
前記受信した電子小切手を前記各利用者の秘密鍵を用いて復号化する小切手復号化手段と、
前記復号化した電子小切手に含まれている前記銀行の署名が正しいことを、前記銀行の公開鍵を用いて確認する署名確認手段と、
前記銀行署名が正しいことが確認されたとき、前記受信した電子小切手を受領したものとして記憶する小切手記憶手段と、
前記小切手記憶手段内の電子小切手を前記他の利用者のＩＣカードへ送信するとき、前記他の利用者のＩＣカードから前記他の利用者の公開鍵を受信する公開鍵受信手段と、
前記小切手記憶手段内の電子小切手を、前記受信した他の利用者の公開鍵によって暗号化する小切手暗号化手段と、
前記暗号化した電子小切手を、前記他の利用者のＩＣカードへ送信する小切手送信手段とを有することを特徴とする電子小切手システム用のＩＣカード。

【請求項11】 請求項10記載のICカードにおいて、電子小切手には、一定の順序で並んだ複数の数字が含まれており、前記各利用者のICカードが、前記他の利用者のICカードから前記電子小切手を受信するとき、第1の乱数を発生させて前記他の利用者のICカードに送信する乱数発生手段と、前記受信した電子小切手に含まれている前記複数の数字の順序が、前記通知した第1の乱数に従って一定の規則の下で正しく変更されていることを確認する数字順序確認手段と、前記小切手記憶手段内の電子小切手を、前記銀行コンピュータ及び他の利用者のICカードのいずれかである受領者装置へ送信するとき、前記受領者装置が発生させた第2の乱数を前記受領者装置から受信する乱数受信手段と、前記小切手記憶手段内の電子小切手に含まれている前記複数の数字を、前記受信した第2の乱数に従って前記一定の規則の下で変更する順序変更手段とを更に有し、前記各利用者のICカードの前記小切手記憶手段が、前記銀行署名が正しいことが確認されたのに加え、前記受信した電子小切手の数字順序が正しく変更されていることが確認されたとき、前記受信した電子小切手を受領したものとして記憶することを特徴とする電子小切手システム用のICカード。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、通信ネットワークを通じた商取引（電子商取引という）に適用される電子小切手システムの改良に関するものである。

【0002】

【従来の技術】従来、商取引においては、現金や手形、小切手のように特定の紙類や金属類等に貨幣価値を化体させた物理的媒体をベースとして、決済が行われてきた。

【0003】しかし、近年、通信ネットワークの急速な発達によって、あらゆる情報の授受が通信ネットワークを通じて行われるようになり電子商取引と称される、通信ネットワークを通じた商取引が実現可能になると、電子商取引の当事者間において上記物理的媒体の占有を移転する方法以外の決済方法が必要になってくる。

【0004】そこで、図1に示すような電子小切手システムが、特開平6-162059号公報において開示され、この電子小切手システムに関して検討が行われている。

【0005】

【発明が解決しようとする課題】ところで、上記電子小切手システムにおいては、電子小切手は単なる「0」と「1」とのビット列で表される情報になってしまう。そ

のため、それら情報のコピーや偽造をどのような方法で防止するのか、及び、取引の相手方の確認や電子小切手の授受等が暗号技術によって行われる際に、使用される鍵の管理の安全性をどのような方法で確保するのが最も重要な問題になってくる。

【0006】例えば、上記システムを示した図1において、支払者3が通信ネットワークを通じて銀行1に、1万円の電子小切手の発行依頼を送信したとする。銀行1ではこの発行依頼を受信すると、支払者3の口座から1万円を引き落とすと共に、支払者3に、電子小切手で1万円を支払うこととなる。

【0007】この電子小切手による支払に際して、銀行1から通信ネットワークを通じて送信されてくる1万円の情報が、仮に支払者3にも解読できない態様で暗号化されていたとしても、支払者3がこの情報を受信したままの態様でコピーすることは極めて簡単に行える。しかも、支払者3にはこの情報の中身が判らなかつたとしても、この情報が1万円の価値があることが判っている。

【0008】そのため、支払者3は、この1万円の電子小切手をコピーしておき、商店5に対する支払いだけでなく商店7に対する支払いに使用しても、商店7ではその電子小切手がコピーされたものか否かの判定は行えない。また、商店5もこの電子小切手をコピーして、他者（図示しない）への支払いに重複使用することが可能である。

【0009】そこで、上記システムでは同一電子小切手の2重使用を防止するための方法として以下のような対策を講じている。即ち、発行済み電子小切手を一元的に登録する証明機関を設け、この証明機関に通信ネットワークを通じて電子小切手を格納した金銭モジュールを定期的にアクセスさせて電子小切手の重複使用や不正使用のチェックを受けるよう、電子小切手所有者に義務付けている。

【0010】しかし、この方法では、不特定多数の個人が電子小切手を所有するようになると、証明機関の負荷が非常に大きくなる。また、電子小切手の使用が証明機関の運転時間によって制約を受けたり、仮に証明機関が24時間運転を行っている場合でも証明機関がダウンしたときは、電子小切手不能使用という問題点が生ずる。更に、不特定多数の個人が比較的低い金額の電子小切手の授受を多数回行うような場合には、証明機関に対する通信コストの負担割合が増大するという問題点も生ずる。

【0011】従って本発明の第1の目的は、電子小切手所有者が多数存在するシステムにおいて、取引の当事者間だけの通信（つまり、オフライン通信）で電子小切手のコピー使用の検出ができ、受領した電子小切手で他者にも支払いが行える電子小切手システムを提供することにある。

【0012】また、本発明の第2の目的は、取引の相手

方の確認や電子小切手の授受等が暗号技術によって行われる際に、使用される鍵の管理が安全、容易で且つ、振出人の署名の確認が行える電子小切手システムを提供することにある。

【0013】

【課題を解決するための手段】本発明の第1の側面に従う電子小切手システムは、電子小切手の振出し及び決済を行う銀行のコンピュータと、その電子小切手を利用する複数の利用者の各々が所持するICカードとを備える。銀行コンピュータは、電子小切手を振出すとき、その電子小切手にその銀行の電子署名を付与する。各利用者のICカードは、それぞれの利用者の秘密鍵及び公開鍵と、銀行の公開鍵とを記憶している。各利用者の秘密鍵は、それぞれのICカード外へ漏れることはないよう、ICカード内で秘密に保持されている。

【0014】各利用者が銀行又は他の利用者から電子小切手を受領するときは、当該利用者のICカードが、その小切手支払者の装置つまり銀行コンピュータ又は他の利用者のICカードと通信可能に接続され、そして、その支払者装置に対し当該利用者の公開鍵を送信し、且つ、その支払者装置から前記電子小切手を受信する。次に、当該利用者のICカードは、受信した電子小切手を当該各利用者の秘密鍵を用いて復号化し、続いて、その復号化した電子小切手に含まれている銀行署名が正しいことを、その銀行の公開鍵を用いて確認する。その結果、銀行署名が正しいことが確認されると、その受信した電子小切手を正式に受領して記憶する。

【0015】一方、各利用者が電子小切手を他の利用者へ渡そうとする時は、当該利用者のICカードは相手のICカードと通信可能に接続され、そして、まず、その相手ICカードからその相手の公開鍵を受信し、次に、その受信した相手の公開鍵を用いて送信対象の電子小切手を暗号化し、そしてこの暗号化した電子小切手を相手カードへ送信する。相手カードは、上記した小切手受領時の動作と同じ処理を行うことにより、その送信された電子小切手の署名の正当性を確認し、そして正式に受領する。

【0016】このように、本システムでは、電子小切手を授受するときの鍵の通信は、小切手授受を行う当事者が、第3者と通信することなしに、各々の公開鍵を相手に通知するだけで済むため、鍵の管理が容易である。

【0017】また、本発明の第2の側面に従う電子小切手システムは、電子小切手の振出し及び決済を行う銀行のコンピュータと、その電子小切手を利用する複数の利用者の各々が所持するICカードとを備える。銀行コンピュータは、電子小切手を振出すとき、その電子小切手に一定の順序で並んだ複数の数字を付与する。また、各利用者のICカードは、他の利用者のICカードから電子小切手を受信するとき、まず乱数を発生させて相手のICカードに送信する。相手のICカードは、その乱数

に応じて、送信対象の電子小切手内の複数数字の順序を一定の規則の下で変更し、その後、その電子小切手を当該利用者のICカードへ送信する。当該利用者のICカードは、相手から受信した電子小切手内の複数数字の順序が、自分が相手に送った乱数に従って正しく変更されているか否かをチェックし、正しいことが確認された場合にのみ、その電子小切手を正式に受領する。

【0018】このようにすると、もし、ある利用者が過去の支払で送信済みの電子小切手をコピーしておき、このコピーを別の支払の為に再度送信した場合、そのコピーに含まれている複数数字の順序は過去の送信時の乱数に基づいて変更されたものであるから、今回の送信時の乱数に基づく順序とは異なることになる。よって、そのコピーの受領は拒否され、電子小切手の不法な二重使用が防止される。

【0019】好適な実施形態では、上記2つのシステムの双方の構成が組み合わされる。この実施形態では、銀行コンピュータが利用者のICカードから電子小切手を受け取るときも、上述した利用者ICカード同士の電子小切手授受のときと同様の態様で、受け取った電子小切手の署名確認と数字列順序の確認とを行なう。

【0020】

【実施の形態】まず、本発明の電子小切手システムの原理的背景について説明する。

【0021】この種の電子小切手システムでは暗号処理は必須であり、特に、本発明に係るシステムでは、通信文を暗号化するだけでなく通信文に署名（電子署名）を施し、相手（即ち、送信元）を確認する機能を有する公開鍵暗号方式が用いられている。

【0022】この公開鍵暗号方式を利用して相手を確認する方式は、特開昭60-26378号（デジタル署名方式）等に開示されている通りである。即ち、原理的には送信者側が通信文を圧縮し、この圧縮したデータに対し秘密鍵によって復号化処理を行い、これを認証子として通信文と共に相手方（受信者側）に送る。その通信文及び認証子を受け取った相手方は、その認証子を相手の公開鍵で暗号化した結果と、通信文を送信者側で圧縮したのと同じ方法で圧縮した結果とが同一であるかどうかをチェックする。これによって上記通信文が正しい相手から（秘密鍵を有している相手から）送信されたものであることを確認することができる。

【0023】次に、上述した原理を、本発明の一実施形態に係る電子小切手システムを示す図2を参照して具体的に説明する。この図2では、簡単のため、電子小切手システムの構成要素を単純化して示している。

【0024】上記システムは、図示のように、サービス享受者（例えば買物客）11、銀行15、サービス享受者11の銀行口座17、銀行15の払出小切手支払口座21、サービス提供者（例えば商店）27、及びその銀行口座35から構成される。サービス享受者11及びサ

ービス提供者27は、それぞれICカード(図示しない)を所有し、それらICカードが電子小切手や秘密鍵及び公開鍵等を所持するための媒体として用いられる。

【0025】図2において、まず、サービス享受者11が、矢印13で示すように銀行15に対し電子小切手の振出しを依頼すると、銀行15は、サービス享受者11から要求された金額以上の残高が口座17にあるか否かを確認する。この結果、上記残高が口座17にあれば、要求金額を矢印19で示すように口座17から銀行15の払出小切手支払口座21に移すと共にサービス享受者11に対し、矢印23で示すように銀行振出の電子小切手を発行する。

【0026】サービス享受者11は、この振出された電子小切手の正当性が確認できたならば、この電子小切手を受領する(ここで、銀行振出の小切手とする理由は、暗号鍵の管理を容易にすると共に、この小切手により支払いを受ける者に対して支払保証を確実にするという目的があるためである)。

【0027】次に、サービス享受者11は、矢印25で示すようにサービス提供者27からサービスの提供を受けたり商品の購入等を行って、それらの購入代金を矢印29で示すようにサービス提供者27に対し電子小切手で支払う。サービス提供者27は、この電子小切手が銀行振出の正当な小切手であることが確認できたならば、この電子小切手を受領する。その後、サービス提供者27は、矢印31で示すように銀行15に対し、サービス享受者11から受領した電子小切手を呈示し、支払を要求する。

【0028】銀行15は、サービス提供者27が呈示した電子小切手の正当性を確認し、その結果、自己振出の電子小切手であることが確認できたならば、矢印33で示すように額面金額を払出小切手支払口座21からサービス提供者27の口座5に振替える。

【0029】上述した電子小切手システムを実現するには、銀行15、サービス享受者11、サービス提供者27が夫々秘密鍵と公開鍵とを所有し、取引の都度相手の署名を確認する必要がある。また、自己の秘密鍵を隠蔽することが重要であると共に、通信相手の公開鍵の入手も容易でなければならない。

【0030】上記システムにおいて、銀行15は通常、自身の業務を効率的に行うために、コンピュータセンタ(図示しない)を備えている。従って、銀行15の秘密鍵や公開鍵は、そのコンピュータセンタの中に置くこともできる(勿論、この秘密鍵は厳重なる注意を持って管理されなければならない)。しかし、サービス享受者11やサービス提供者27は、その多くが個人であることから、銀行15のようなコンピュータセンタを所有することはできず、その秘密鍵の管理方法が問題となる。

【0031】そこで、サービス享受者11やサービス提供者27には、耐タンパー性(つまり、内部データの不正

法改変が事実上不可能であること)を有するICカードに秘密鍵を格納して所有させることとする。ここで、耐タンパー性を有するICカードとは、少なくともCPU、メモリ、入出力ポート等から構成されるもので、そのメモリには外部から直接アクセスすることができず、メモリに対するアクセスはCPUが制御し、入出力ポートを経由して外部とデータ交換を行う構成のICカードである。

【0032】上述した理由から、サービス享受者11やサービス提供者27は、自身の秘密鍵を格納したICカードを所有する必要があるが、これは以下の方法で入手することができる。

【0033】まず、サービス享受者11やサービス提供者27は、事前に銀行15に夫々口座17、35を開設しておき、銀行15に電子小切手システムを利用する旨の要求を行う。銀行15は、サービス享受者11やサービス提供者27の本人確認や資格確認等を行った後、これら利用者(11、27)の秘密鍵を格納したICカードを発行する。

【0034】これらICカードには、秘密鍵の他、銀行15が発行した正当なICカードだけが有する署名情報や利用者(11、27)のIDや公開鍵、銀行15の公開鍵や銀行15が振出した電子小切手の署名を確認する関数や通信文を暗号化、復号化する関数、受領した電子小切手を格納し管理するための機能等が必要となる。これらの機能は、ICカード内にプログラムとして組込むことで実現できる。

【0035】なお、利用者(11、27)の鍵生成については、銀行15内で利用者(11、27)の秘密鍵、公開鍵を生成することもできるが、銀行15自身が関与しない形で秘密鍵や公開鍵を生成でき、特に利用者(11、27)の秘密鍵については銀行15にも利用者(11、27)本人にも知り得ない形態を取るのが望ましい。この方法としては、ICカード内でCPUが独自に利用者(11、27)の秘密鍵と公開鍵とを生成して公開鍵だけ銀行15に通知する方法がある。また、ICカードの処理能力では鍵生成が困難な場合、銀行15で利用者(11、27)の公開鍵と秘密鍵とを生成させるが、利用者(11、27)の秘密鍵は、ICカードだけに記憶させ、銀行15では保持しないようにしておくことが望ましい。いずれにしても、銀行15のコンピュータセンタが、発行したICカードの利用者ID、及び公開鍵を記憶しておくこととなる。また、利用者(11、27)の秘密鍵は、個々の利用者のICカードのICチップ内に、ICチップ外へ読出すことが不可能な状態で格納される。

【0036】このようにして発行されたICカードを使用して、銀行15とサービス享受者11やサービス提供者27、或いは、サービス享受者11とサービス提供者27との間で電子小切手の授受が行われることとなる。

【0037】まず、図2において、サービス享受者11が銀行15から電子小切手を振出す場合、銀行15は、電子小切手を構成するデータを生成し、これに銀行15の電子署名を付与する。そして、この電子署名を付した電子小切手全体を、サービス享受者11の公開鍵で暗号化した後、サービス享受者11のICカードに送る。サービス享受者11のICカードは、暗号化された電子小切手全体を受け取ると、自身の秘密鍵を使用して復号化し、銀行15の公開鍵を使用して銀行15の証明を確認する。

【0038】このとき、銀行15では、サービス享受者11の利用者IDに基づいてサービス享受者11の公開鍵を検索する必要があるが、公開鍵であるため厳重なセキュリティは要求されない。また、サービス享受者11のICカードは、自身のチップ内に格納された秘密鍵を外部に漏らすことなく上記データを復号化し、自身に記憶されている銀行15の公開鍵を使用して銀行15の電子署名を確認することができる。

【0039】次に、図2において、サービス享受者11が銀行15振出の電子小切手をサービス提供者27に支払う場合について説明する。

【0040】サービス享受者11のICカード及びサービス提供者27のICカードは、夫々銀行15から発行されたときに埋め込まれた正当性を示す銀行15の署名情報や秘密情報を有することを確認することによって相互認証を行う。相互に正当な通信相手であることを確認した2枚のICカードは、互いの公開鍵を交換し合う。サービス享受者11のICカードは、銀行15の電子署名の付いた電子小切手をサービス提供者27の公開鍵で暗号化し、サービス提供者27のICカードに送る。サービス提供者27のICカードは、自身の秘密鍵を外部に漏らすことなく上記データを復号化し、自身に記憶されている銀行15の公開鍵を使用して銀行15の電子署名を確認する。サービス提供者27は、銀行15の電子署名が確認できることでその電子小切手が銀行15から発行されたものであることが確認できる。更に、サービス提供者27は、同様の方法で正当に発行されたICカードを持つ第三者に対し、サービス享受者11から受領した電子小切手で支払いを行うことが可能である。

【0041】ここで、電子小切手の振出人を銀行15としておけば、夫々のICカードに共通的に存在する銀行15の公開鍵を使用して銀行15の電子署名を確認ことができ、鍵の管理が非常に楽になる。なお、電子小切手の振出人を銀行15への要求者であるサービス享受者11とすることもできるが、サービス享受者11の電子署名を確認するためのサービス享受者11の公開鍵を入手する手段が問題となる。

【0042】即ち、サービス享受者11からサービス提供者27にサービス享受者11の公開鍵を渡す場合、サービス享受者11が不正を働き、独自に生成した秘密鍵

と公開鍵とを用いて電子署名を行い、その公開鍵をサービス提供者27に送ったとしても、サービス提供者27はサービス享受者11が不正を働いたかどうか判定することができない。従って、サービス提供者27のICカードは、サービス享受者11と取引する以前にサービス享受者11の公開鍵を所持しているか、銀行15又は公正な第三者機関(図示しない)からサービス享受者11のICカードの公開鍵を入手する必要がある。これは、不特定多数人が取引するシステムでは実現困難である。

【0043】また、社会通念上、不特定多数の個人であるサービス享受者11が振出した小切手よりも、銀行15が振出した小切手の方が信用度が高い。仮に、サービス享受者11とサービス提供者27との間で従来から取引関係があり、サービス享受者11が振出した小切手をサービス提供者27が受け入れたとしても、サービス享受者11振出しの小切手をサービス提供者27が第三者(図示しない)に支払う場合、サービス享受者11と第三者との間で信用関係がなければ、第三者はサービス享受者11振出の小切手を受領することを拒むかもしれない。

【0044】このようにして発行された2枚のICカードを使用して、サービス享受者11やサービス提供者27は、銀行15との間で電子小切手の受領や決済を行うが、これら2枚のICカードと銀行15との間で直接やり取りができる訳ではない。

【0045】これら2枚のICカードと銀行15との間で、電子小切手の受領や決済を行う手段としては、以下のような方法が考えられる。

【0046】(1) 銀行15の窓口上記ICカードを呈示する方法。

【0047】(2) 上記のような電子小切手システムに対応したATMを使用する方法。

【0048】(3) 2枚のICカードと通信を行う機能、2枚のICカードとの間で授受される情報の表示機能、操作者の意思等を2枚のICカードに伝達するための入力機能、及び銀行15と通信を行う機能を少なくとも備える端末機を使用する方法。

【0049】特に(3)の方法では、これに適用される端末機を、市販のパーソナルコンピュータ(パソコン)、ICカードリーダ/ライタ(ICカードR/W)、モデム等を組合せて実現することができるので、サービス享受者11はこの端末機を用いて自宅や勤務先等から電子小切手の受領や決済を行うこともできる。

【0050】更に、(3)の条件を満足するために、持ち運び可能な携帯用端末機と移動体通信とを組合せることで、外出先等からでも電子小切手の受領や決済を行うこともできるようになる。

【0051】また、サービス享受者11とサービス提供者27との間における電子小切手の支払いや受領には、以下のような方法が考えられる。

【0052】(4) サービス提供者27の店舗内に、少なくともサービス享受者11のICカードとサービス提供者27のICカード間での通信機能、情報の表示機能、操作者の意思等を伝えるための入力機能を備えた端末機を使用する方法。

【0053】(5) 上記(3)に示した端末機を使用する方法。

【0054】(6) 上記(4)及び(5)を組合せた端末機を使用する方法。

【0055】(4)の方法は、サービス享受者11がサービス提供者27の店舗に出向き、ここで電子小切手の支払いを行う場合に使用される。

【0056】(5)の方法では、サービス享受者11又はサービス提供者27の一方が遠隔地におり、通信ネットワークを介した状態で電子小切手の支払いが行える。例えば、インターネットを介して情報提供者から有料の情報を受け取り、電子小切手によりその代金の支払いを行う場合等が思料される。

【0057】このように、利用者(サービス享受者11、サービス提供者27)毎の暗号処理に必要な機能をICカード内に組込むことで、上記電子小切手システムに使用する端末機に対し、鍵の管理等に対する要求条件がなくなるため、端末機的设计の自由度が増え、時代の要請にあった電子小切手システムの構築がし易くなる。

【0058】ところで、上記システムにおいては、銀行15から受領した電子小切手がサービス享受者11からサービス提供者27に支払われるとき、サービス提供者27がサービス享受者11以外と通信せずに(つまりオフラインで)、支払われた電子小切手の不正使用をどのように検出するかが、本質的な課題である。

【0059】次に、上記システムにおける発行済み電子小切手の重複使用の防止方法を、図3を参照して説明する。

【0060】図3は、上記電子小切手システムを構成するサービス享受者11、銀行15、及びサービス提供者27を示す拡大図である。図から明らかなように、サービス享受者11は上述した(3)の方法に適用される専用の端末機41及び専用のICカード45を所有し、サービス提供者27も同様の構成の端末機43及び専用のICカード47を所有している。そして、端末機41、43間や端末機41、43と銀行15の端末機との間は、通信ネットワークによって接続可能に構成されているものとする。

【0061】図3において、符号49では、銀行15から振出された例えば1万円の電子小切手はサービス享受者11の公開鍵で暗号化される。この暗号化されたデータは、ICカード45内でサービス享受者11の秘密鍵によって復号化され、サービス提供者27に支払われるとき(符号51で示す)は、サービス提供者27の公開鍵で暗号化される。

【0062】この場合、符号49の時点でのデータを、サービス享受者11本人又は第三者がコピーしておいて、そのままの形でサービス提供者27に支払ってもICカード47は正しいデータに戻すことができないから、この電子小切手の受領は拒否される。なお、サービス享受者11の秘密鍵はICカード45内にあり、ICカード外へは読出し不可能なので、サービス享受者11自身もこの暗号文49を復号化することはできない。

【0063】しかし、符号51の時点でのデータを、サービス享受者11本人又は第三者がコピーしておき、再度サービス提供者27に支払った場合、ICカード47は正しいデータに復号してしまう。ICカード47で、このデータがオリジナルか不法コピーかを判断するためには、過去に受領した電子小切手を記憶しておき、これを検索することが必要となるが、ICカードには無限のメモリを搭載できる訳ではないので、現実的ではない。

【0064】そこで、図4に示すように、銀行15は、1万円の電子小切手を振出す際に、1万円の電子小切手データに値の異なる n 個の乱数 $rbnk1$ 、 $rbnk2$ 、 \dots 、 $rbnkn$ を付与し、サービス享受者11の公開鍵で暗号化し、ICカード45に送信する。

【0065】この暗号化されたデータを受信すると、ICカード45は自身の秘密鍵で復号化して1万円の電子小切手とする。そして、ICカード45はこの電子小切手をICカード47に移すときに、まず、ICカード47から値の異なる n 個の乱数 $rb1$ 、 $rb2$ 、 \dots 、 rbn を貰う。次に、これら乱数 $rb1$ 、 $rb2$ 、 \dots 、 rbn の受信順序(並び順序)と大きさによって銀行15で付与された $rbnk1$ 、 $rbnk2$ 、 \dots 、 $rbnkn$ の並びを一定の規則で変更する。その後、サービス提供者27の公開鍵で暗号化し、ICカード47へ送信する。

【0066】ICカード47では、ICカード45から受信した電子小切手データを復号化した後、自分が送信した乱数の順序と大きさの関係と $rbnk1$ 、 $rbnk2$ 、 \dots 、 $rbnkn$ の並び順の関係が規則に従って変更されているか否か进行检查し、規則に従っていないときは、この電子小切手の受領を拒否する。従って、サービス享受者11がICカード45から出力された符号51の時点でのデータをコピーしておいても、ICカード47から発生する乱数 $rb1$ 、 $rb2$ 、 \dots 、 rbn の順序と大きさとの関係がコピーした時点と一致しない限り使用することができない。

【0067】ここで、符号51の時点でのデータをコピーしたサービス享受者11がサービス提供者27と正常に取引できる確率は、 $1/n!$ である。具体例を示せば下記の通りであるから、乱数の数 n は、7個程度以上あれば実用上問題ないであろう。

【0068】

確率 (n=5) = $1/5! = 1/120 \approx 0.83\%$
 確率 (n=6) = $1/6! = 1/720 \approx 0.14\%$
 確率 (n=7) = $1/7! = 1/5040 \approx 0.02\%$
 確率 (n=8) = $1/8! = 1/40320 \approx 0.002\%$
 確率 (n=9) = $1/9! = 1/362880 \approx 0.0003\%$

なお、図示のシステムでは、 $rbnk1 \sim rbnkn$ は、5個の乱数とし、 $rbnk1 \sim rbnk5$ の大小関係は $rbnk1 < rbnk2 < rbnk3 < rbnk4 < rbnk5$ としてある。ICカード45は、ICカード47から $rb1, rb2, rb3, rb4, rb5$ の順で乱数を受信する。そして、 $rb1=1, rb2=4, rb3=2, rb4=5, rb5=3$ であるとする。ICカード45は、上記乱数を $rbnk1, rbnk4, rbnk2, rbnk5, rbnk3$ の順に並び変えてICカード47に送信する。

【0069】次に、上記システムを利用するのに必要な電子小切手台帳（つまり、ICカード）の発行手順を、図5のフローチャートを参照して説明する。

【0070】電子小切手の利用者であるサービス享受者11及びサービス提供者27は、銀行15から電子小切手台帳としてのICカードを発行して貰う必要がある。銀行15がサービス享受者11にICカードを発行する際の手順を以下に示す。この手順はサービス提供者27にICカードを発行する際にも適用される。

【0071】まず、ICカード発行の準備として、電子小切手の発行銀行となる銀行15は、電子小切手の署名に必要な公開鍵 K_{PBNK} と秘密鍵 K_{SBNK} とを生成しておき、公開鍵 K_{PBNK} を公開しておく。また、秘密鍵 K_{SBNK} については、厳重な管理の下に置かれるようにしておく。

【0072】ステップS101において、サービス享受者11は銀行15に対し、ICカードの発行を要求し、この要求を受けると銀行15は、ステップS102においてサービス享受者11の本人確認を行い、要求者がサービス享受者11本人であれば、サービス享受者11の口座の有無を調べる。サービス享受者11が口座を持っていない場合は口座を開設させる。なお、銀行15がサービス享受者11に対して本人確認を行う方法は、免許証等の公的証明書、銀行15発行の通帳と印鑑、暗証番号等の本人しか知らない秘密情報を知っていることによる確認、声紋、指紋等による生物学的特徴を利用した方法等を単独又は組合せて行う。

【0073】次に、ステップS103において、銀行15はサービス享受者11のために発行するICカード45に対し、自身の公開鍵 K_{PBNK} 、秘密鍵 K_{SBNK} 、利用者ID (IDa) を通知する。そして、ICカード45に対し、サービス享受者11個人の公開鍵 K_P と秘密鍵 K_S の発行、及び利用者ID (IDa) と公開鍵 K_P に対する署名 Sa の生成を依頼する。なお、ICカード45は、署名 Sa を生成後、銀行15の

秘密鍵 K_{SBNK} は破棄する。ICカード45に鍵生成能力が無い場合には、公開鍵 K_P 及び秘密鍵 K_S の生成や公開鍵 K_P に対する署名 Sa の生成は銀行15のセンタで行う。

【0074】次に、ステップS104において、鍵の生成依頼を受けたICカード45は、サービス享受者11個人の公開鍵 K_P と秘密鍵 K_S とを生成した後、利用者ID (IDa) と公開鍵 K_P に対する署名 Sa とを、銀行15の秘密鍵 K_{SBNK} により生成する。ICカード45は、 K_{PBNK} 、 K_S 、 K_P 、 IDa 、 Sa を記憶すると共に、銀行15に対して公開鍵 K_P を通知する。なお、ICカード45で個人の公開鍵、秘密鍵を生成する場合は、鍵生成依頼時の日付時刻、乱数等を使用して同じ鍵が生成されないようにする必要がある。

【0075】次に、ステップS105において、銀行15は、 IDa と公開鍵 K_P を記憶しておく。

【0076】次に、上記のようにして発行されたICカードを用いて行われる電子小切手の振出しを、図6、及び図7のフローチャートを参照して説明する。

【0077】図6、及び図7は、サービス享受者11が銀行15に対して、電子小切手の振出しを依頼する場合の手続を示す。

【0078】まず、ステップS111において、サービス享受者11は、ICカード45が使用できる銀行15のATM又は銀行15と通信ネットワークを通じて通信が可能で且つ電子小切手台帳であるICカード45が使用できる端末機41を経由して、銀行15に対し電子小切手の振出依頼を行う。なお、ICカード45とサービス享受者11及び銀行15とは実際にはATM又は端末機41を介して通信を行うがこれらの装置は情報を中継するだけであるため、以降の説明からは省略する。

【0079】次に、ステップS112において、振出要求を受けたICカード45は、サービス享受者11に対してサービス享受者11の本人確認を行う。本人確認の方法は、暗証番号、声紋、指紋等による生物学的特徴を利用した方法等を単独又は組合せて行う。その後、ステップS113において、ICカード45は本人確認が行えたならば、銀行15に対し、 IDa からの電子小切手振出し要求を通知する。

【0080】次に、ステップS114において、ICカード45と銀行15は、相互に認証を行い、互いに正当な通信相手であることを確認する。例えば、ここでは、次のような方式で相互の認証を行うことが可能である。ICカード45は、 K_S 、 IDa 、 Sa を銀行15の

公開鍵KPBKで暗号化し、銀行15に送信する。銀行15は、自身の秘密鍵KSBKでこのデータを復号化した後、自身の公開鍵KPBKにより署名Saを検査することにより、ICカード45が正当に発行されたものであることを確認する。また、銀行15は、例えば公開鍵KPBKと受信したIDaとに対し、自身の秘密鍵KSBKで署名を行い、この署名情報だけをICカード45に送信する。ICカード45では、この署名を公開鍵KPBKで元に戻し、公開情報であるKPBKと自身のIDaであることとを検証することにより、署名情報の送信元が正当な銀行15であることを確認する。

【0081】このようにして相互認証を行った後、ステップS115において銀行15は、乱数raを生成し、一方向性の暗号関数fと電子小切手台帳発行時に生成したサービス享受者11の公開鍵KPAとにより下記の態様でraを暗号化し、ICカード45に送信する。

【0082】 $Era = f(ra, KPA)$

その後、ステップS116において、ICカード45は、受信したEraを自分の秘密鍵KSAにより下記のように復号化し、サービス享受者11に対し電子小切手の振出金額等の入力を要求する。

【0083】 $ra = f^{-1}(Era, KSA)$

ここでの f^{-1} は、関数fの逆関数を示す。以下、この明細書において同様の表現は逆関数を示す(但し、各図中では、例えばfの-1乗のような表現により逆関数を示している)。

【0084】次に、ステップS117において、サービス享受者11は、振出して貰いたい電子小切手の金額と枚数とをICカード45に通知する。ここでは、5000円の電子小切手1枚を振出す例で考える。

【0085】ステップS118において、ICカード45は、銀行15に対し電子小切手の振出しを要求する通信文を生成する。この通信文には少なくとも、ステップS116において復号化したra、振出要求金額5000円、振出枚数1枚、電子小切手台帳発行時に格納されたID番号(IDa)のデータを含む。

【0086】更に、ステップS119において、ICカード45ではステップS118で生成した通信文を元に一方向性関数Dと秘密鍵KSAとを使用して、メッセージ認証子MACaを生成する。

【0087】 $MACa = D(5000円、1枚、ra、IDa、\dots、KSA)$

ここで生成したMACaを、ステップS118において生成した通信文に付加する。この実施形態において、上記関数の処理(認証子を求める)は、図8に示すような態様で行う。

$MACbnk1 = H(5000円、振出銀行名、振出日時、\dots、rbnk5、KSBK)$

$MACbnk2 = H(5000円、振出銀行名、振出日時、\dots、rbnk2$

【0088】そして、ステップS120において、ステップS119で生成した通信文+MACaを一方向性の暗号関数Freq及び公開鍵KPBKで下記のように暗号化し、これを銀行15に送信する。

【0089】 $Ereq = Freq(5000円の電子小切手1枚の振出要求通信文+MACa、KPBK)$

この実施形態において、上記関数の処理(暗号化/復号化を行う場合)は、図9に示すように暗号化することを示す。また、この実施形態において、+の演算子は、図9に示すようにデータを連結することを示す。

【0090】次に、ステップS121において、暗号文Ereqを受信した銀行15は、自身の秘密鍵KSBKにより下記のようにEreqを復号化する。

【0091】5000円の電子小切手1枚の振出し要求通信文+MACa= $Freq^{-1}(Ereq、KSBK)$

次に、ステップS122において、復号化した通信文の中からステップS115で生成したra、振出し要求金額5000円、振出枚数1枚、電子小切手台帳発行時に格納されたID番号(IDa)のデータを取り出し、MACaが正しいことを検証する。

【0092】この検証は、 $MACa^{-1} = D(5000円、1枚、ra、IDa、\dots、KPA)$ と、5000円の電子小切手1枚の振出要求通信文+MACa= $Freq(Ereq、KSBK)$ とを比較することによって行われる。次に、ステップS123において、認証子MACaが正しいことを確認した銀行15は、サービス享受者11の口座17に振出金額合計以上の残高があることを確認し、提出金額、提出銀行名、提出日時等から成る電子小切手の通信文を要求された振出枚数の通信文を要求された振出枚数分生成させる。この場合、振出枚数は1枚のため通信文は1つとなる。

【0093】次に、ステップS124において、1つの通信文についてN個の乱数rbnk1~rbnkNを発生させる。但し、乱数rbnk1~rbnkNは、すべて異なる値となるように生成する。ここでは、取り敢えず5個の乱数を発生させることとし、発生した乱数rbnk1~rbnk5の大小関係は、 $rbnk1 < rbnk2 < rbnk3 < rbnk4 < rbnk5$ の関係があるものとする。そして、通信文の中から少なくとも振出金額、振出銀行名、提出日時を取り出し、これらのデータに乱数rbnkNを付加し、一方向性関数Hと銀行15の秘密鍵KSBKとにより下記のようにN個のメッセージ認証子MACbnk1~MACbnkNを求める。

【0094】

、KSBNK)

$MACbnk5 = H(5000円、振出銀行名、振出日時、\dots、rbnk5、KSBNK)$

更に、ステップS125において、ステップS123で生成した通信文にステップS124で発生した乱数と認証子を付加し、一方向性関数Fchrとサービス享受者11の公開鍵KPAとで下記のように暗号文Echrを生成する。ここで、乱数rbnkと認証子MACbnkは対応が取れるように並べるものとする。

【0095】 $Echr = Fchr(5000円の電子小切手の振出許可通知文 + rbnk1 + MACbnk1 + rbnk2 + MACbnk2 + \dots + rbnk5 + MACbnk5)$

そして、ステップS126において、このEchrをサービス享受者11のICカード45へ送信すると共に、サービス享受者11の口座17から当該金額（ここでは5000円）を引き落とし、自行の払出小切手支払いに

$MACbnk1 = H(5000円、振出銀行名、提出日時、\dots、rbnk1、KPBNK)$

$MACbnk2 = H(5000円、振出銀行名、提出日時、\dots、rbnk2、KPBNK)$

$MACbnk5 = H(5000円、振出銀行名、提出日時、\dots、rbnk5、KPBNK)$

上記によって得られたMACbnk1～MACbnk5とステップS127でEchrを復号化(Fchr*(Echr, KSA))した結果に含まれるMACbnk1～MACbnk5が同一であれば、この認証子は銀行15によって署名されたものと判定する。

【0098】次に、ステップS129において、ICカード45は、ステップS128によって銀行15からの「5000円の電子小切手の振出許可通知文」が確認できれば、5000円の電子小切手の振出許可通知文+rbnk1+MACbnk1+rbnk2+MACbnk2+……+rbnk5+MACbnk5を電子小切手としてICカード45内に格納しておく。

【0099】次に、サービス享受者11からサービス提供者27に対する電子小切手での支払手順について説明する。

【0100】図10、及び図11は、サービス提供者27からサービス、商品等の提供を受けたことに対する代金の支払を電子小切手で行う場合の手順を示すフローチャートである。この電子小切手での支払を行う前提として、サービス提供者27についてもサービス享受者11におけると同様に、図5～図7で示した手順によって銀

当てる口座21に入金しておく。その後、ステップS127において、ICカード45は銀行15から受信したEchrを自身の秘密鍵KSAによって復号化する。

【0096】5000円の電子小切手の振出許可通知文+rbnk1+MACbnk1+rbnk2+MACbnk2+……+rbnk5+MACbnk5)=Fchr*(Echr, KSA)

次に、ステップS128において、「5000円の電子小切手の振出許可通知文」の中から振出金額、振出銀行名、振出日時等を取り出し、銀行BNKの公開鍵KPBNKを使用してMACbnk1～MACbnk5の署名が確かに銀行BNKによって行われたものであることを確認する。

【0097】

行15が発行したICカード47を所持しているものとする。従って、ICカード47にもICカード45と同様、銀行15の公開鍵KPBNK、サービス提供者27の秘密鍵KSB、サービス提供者27の公開鍵KPB、サービス提供者27の利用者ID(IDb)、利用者ID(IDb)と公開鍵KPBに対する銀行15の署名Sbが記憶されている。また、この例では、サービス享受者11が図7のステップS129でチャージした電子小切手で支払うものとする。

【0101】まず、ステップS131において、サービス提供者27はサービス享受者11にサービス又は商品を提供したことに対する代金支払の請求を行う。次に、ステップS132において、サービス享受者11はICカード45に対し電子小切手の払出指示を行う。その後、ステップS133において、電子小切手払出指示を受けたICカード45は、サービス享受者11に対してサービス享受者11の本人確認を行う。本人確認の方法は、暗証番号、声紋、指紋等による生物学的特徴を利用した方法等を単独又は組合せることによって行う。この本人確認の後、ステップS134において、ICカード45は自カード内に格納している電子小切手の金額、枚

数、合計金額等をサービス享受者11に通知すると共にいくら払出すのか、又は、どの電子小切手を払出すのかをサービス享受者11に問い合わせる。

【0102】次に、ステップS135において、サービス享受者11は、いくら払出すのか、又は、どの電子小切手を払出すのかをICカード45に指定する。ここでは、ステップS129でチャージした電子小切手を払出すこととする。次に、ステップS136において、指定を受けたICカード45は、金額で指定をされた場合は指定金額以上の残高の電子小切手があることを確認すると共に、ICカード47に対し電子小切手により支払を行う旨の通知を行う。次に、ステップS137において、ICカード45とICカード47は相互に認証を行うことにより、互いに正当な通信相手であることを確認する。例えば、次のような方法で互いの認証と公開鍵の交換とを行う。ICカード45は、KSA、IDa、SaをICカード47へ送信する。ICカード47では、銀行125の公開鍵KPBKにより署名Saを検証することによって、ICカード45が銀行15により発行されたものであり、且つ、KSA、IDaが正しいことを確認することができる。また、ICカード47から同様にKSB、IDb、SbをICカード45に送信することで、ICカード45は、ICカード47、及びその公開鍵KPBの正当性を検証することができる。

【0103】次に、ステップS138において、ICカード47は、N個の乱数rb1～rbnを生成する。このとき生成する乱数の個数は、図6のステップS124で生成した乱数の個数と同じ数を生成するものとし、生成した乱数はすべて異なる値になるよう生成する。この例では、5個の乱数rb1～rb5を生成し、rb1、rb2、rb3、rb4、rb5の順に並べ、一方方向性関数frと公開鍵KPAとで下記のように暗号化してICカード45に送信する。

【0104】 $Erb = fr(rb1 + rb2 + rb3 + rb4 + rb5, KPA)$

なお、この例では、rb1～rb5の大小関係をrb1<rb3<rb5<rb2<rb4とする。

【0105】次に、ステップS139において、ICカード45はErbを復号化し、rb1～rb5と自身のIDa等から一方方向性関数Gを、また、秘密鍵KSAから認証子MACaを、夫々下記のように生成する。

【0106】 $rb1 + rb2 + rb3 + rb4 + rb5 = fr * (Erb, KSA)$

$MACa = G(rb1, rb2, rb3, rb4, rb5, IDa, \dots, KSA)$

次に、ステップS140において、ステップS139で格納した電子小切手「5000円の電子小切手の振出許可通知文+rbnk1+MACbnk1+rbnk2+MACbnk2+…+rbnk5+MACbnk5」を取出し、受信した乱数rb1～rb5の大小関係の順に

$rbnk1 + MACbnk1 \sim rbnk5 + MACbnk5$ を並べ変える。この例においては、乱数rbnk1～rbnk5の大小関係は、ステップS124で示した通りrbnk1<rbnk2<rbnk3<rbnk4<rbnk5であるから、

5000円の電子小切手の振出許可通知文+rbnk1+MACbnk1+rbnk4+MACbnk4+rbnk2+MACbnk2+rbnk5+MACbnk5+rbnk3+MACbnk3と並べ変える。

【0107】今、ICカード47から送信されてきた乱数は、rb1<rb3<rb5<rb2<rb4であるから、仮に、rb1=1、rb2=4、rb3=2、rb4=5、rb5=3とすると、銀行15から受領したrbnk1～rbnk5は、rbnk1<rbnk2<rbnk3<rbnk4<rbnk5となる。よって、これをrbnk1、rbnk4、rbnk2、rbnk5、rbnk3の順に並べ変えることとなる。

【0108】次に、ステップS141において、ステップS140で並べ変えた電子小切手に、ステップS139で生成したMACaとIDaとを加え、一方方向性関数Fpayとサービス提供者27の公開鍵KPBとで下記のように暗号文Epayを生成する。

【0109】 $Epay = Fpay(5000円の電子小切手の振出許可通知文 + rbnk1 + MACbnk1 + rbnk4 + MACbnk4 + rbnk2 + MACbnk2 + rbnk5 + MACbnk5 + rbnk3 + MACbnk3 + MACa + IDa, KPB)$

次に、ステップS142において、ICカード45は、ICカード47に暗号文Epayを送信する。ICカード45は、暗号文Epayが正常にICカード47に届いたことが確認されれば、送信した電子小切手「5000円の電子小切手の振出許可通知文+rbnk1+MACbnk1+rbnk2+MACbnk2+…+rbnk5+MACbnk5」を無効化する。

【0110】次に、ステップS143において、暗号文Epayを受信したICカード47は、秘密鍵KSBにより暗号文Epayを復号化する。

【0111】5000円の電子小切手の振出許可通知文+rbnk1+MACbnk1+rbnk4+MACbnk4+rbnk2+MACbnk2+rbnk5+MACbnk5+rbnk3+MACbnk3+MACa+IDa=Fpay*(Epay, KSB)

暗号文Epayを復号化した後、ステップS144において、ICカード47はステップS138で生成した乱数rb1～rb5、IDa等からICカード45の公開鍵KPAと署名を行うための一方方向性関数Gとから下記のようにしてICカード45の署名を確認する。

【0112】 $MACa' = G(rb1, rb2, rb3, rb4, rb5, IDa, \dots, KPA)$

そして、MACa^{*}とステップS143で得られたMACaとを比較し、同一であればICカード45による署名がされたものであると認識する。

【0113】次に、ステップS145において、ステップS138でICカード45に送信した乱数rb1~rb5の大小関係から、ステップS143で暗号文Epayを復号化した際に得られたrbnk1~rbnk5の大小関係の並びが正しいことを確認する。この例では、送信したrb1~rb5の大小関係がrb1<rb3<rb5<rb2<rb4であったため、rbnk1~rbnk5がrbnk1、rbnk4、rbnk2、rbnk5、rbnk3の順序で並んでいることを確認する。もし、ここで乱数rbnk1~rbnk5の並び順

MACbnk1^{*}=H(5000円、振出銀行名、振出日時、…、rbnk1、KPBK)
MACbnk4^{*}=H(5000円、振出銀行名、振出日時、…、rbnk4、KPBK)

MACbnk3^{*}=H(5000円、振出銀行名、振出日時、…、rbnk3、KPBK)

上記によって得られたMACbnk1^{*}~MACbnk5^{*}と、ステップS143でEpayを復号化(Fpay*(Epay、KSB))した結果に含まれるMACbnk1~MACbnk5とが同一であれば、この認証子は銀行15によって署名されたものと判断する。

【0116】次に、ステップS147において、銀行15の署名が確認されれば、ICカード47は受領した電子小切手の金額をサービス提供者27に通知する。そして、5000円の電子小切手の振出許可通知文+rbnk1+MACbnk1+rbnk4+MACbnk4+rbnk2+MACbnk2+rbnk5+MACbnk5+rbnk3+MACbnk3を電子小切手として格納する。

【0117】次に、サービス提供者27が銀行15に対し、上記電子小切手を用いて決済を行う手順について説明する。

【0118】図12、及び図13は、サービス提供者27がサービス享受者11から受領した5000円の電子小切手を銀行15に呈示し、決済を行う際の手順を示すフローチャートである。

【0119】まず、ステップS151において、サービス提供者27は、電子小切手台帳であるICカード47が使用できる銀行15のATM又は銀行15と通信が可能で、且つ、電子小切手台帳であるICカード47が使用可能な端末機を経由してICカード47に対し電子小切手の決済要求を行う。

【0120】次に、ステップS152において、電子小切手払出指示を受けたICカード47は、サービス提供

がステップS138でICカード45に送信した順序と異なっていた場合は、銀行15が正当に発行したICカード45の中から送信されたものではなく不正使用された電子小切手であるとしてサービス提供者27に通知すると共に以降の支払手順を停止する。

【0114】更に、次のステップS146において、ICカード47は「5000円の電子小切手の振出許可通知文」の中から振出金額、振出銀行名、振出日時等を取り出し、振出銀行名から自身が記憶している銀行15の公開鍵KPBKを得る。そして、この公開鍵KPBKを使用してMACbnk1~5の署名が確かに銀行15によって行われたものであることを確認する。

【0115】

者27に対してサービス提供者27の本人確認を行う。本人確認の方法は、暗証番号、声紋、指紋等による生物学的特徴を利用した方法等を単独又は組合せることにより行う。

【0121】この本人確認の後、ステップS153において、ICカード47は自カード内に格納している電子小切手の振出銀行、提出日、金額、枚数、合計金額等をサービス提供者27に通知すると共に、どの電子小切手を決済するのかをサービス提供者27に問い合せる。次に、ステップS154において、サービス提供者27は決済する電子小切手をICカード47に指定する。ここでは、サービス享受者11から支払を受けた銀行15振出の5000円の電子小切手(図10及び図11参照)の決済を行うものとする。次に、ステップS155において、指定を受けたICカード47は、銀行15に対し電子小切手の決済を行う旨の通知を行う。

【0122】その後、ステップS156において、ICカード4と銀行15とは、相互に認証を行うことにより互いに正当な通信相手であることを確認する。ここでは、図6のステップS114と同様にICカード47からは、KSB、IDb、Sbを銀行15に送信する。また、銀行15は、公開鍵KPBKと受信したIDbに対し、自身の秘密鍵KSBKで署名を行い、この署名情報だけをICカード47に送信することで相互の認証を行うことができる。

【0123】次に、ステップS157において、銀行15は、N個の乱数rg1~rgnを生成する。このとき生成する乱数の個数は、ステップS124で生成した乱

数の個数と同じ数を生成するものとし、生成した乱数はすべて異なる値になるように生成する。この例では、5個の乱数 $rg1 \sim rg5$ を生成し、 $rg1$ 、 $rg2$ 、 $rg3$ 、 $rg4$ 、 $rg5$ の順に並べ、一方向性関数 frg と公開鍵 KPB とで下記のように暗号化して、順にICカード47に送信する。

【0124】 $Erg = fr(rb1 + rb2 + rb3 + rb4 + rb5, KPA)$

なお、この例では、 $rg1 \sim rg5$ の大小関係を $rg4 < rg1 < rg2 < rg5 < rg3$ とする。

【0125】次に、ステップS158において、ICカード47は Erg を復号化し、受信した $rg1 \sim rg5$ と自身の IDb 等から一方向性関数 G を、秘密鍵 KSB から認証子 $MACb$ を、夫々下記のように生成する。

【0126】 $rb1 + rb2 + rb3 + rb4 + rb5 = fr * (Erb, KSA)$

$MACb = G * (rg1, rg2, rg3, rg4, rg5, IDb, \dots, KSB)$

次に、ステップS159において、ステップS157で格納した電子小切手「5000円の電子小切手の振出許可通知文+ $rbnk1 + MACbnk1 + rbnk2 + MACbnk2 + \dots + rbnk5 + MACbnk5$ 」を取出し、受信した乱数 $rg1 \sim rg5$ の大小関係の順に $rbnk1 + MACbnk1 \sim rbnk5 + MACbnk5$ を並べ変える。この例においては、 $rbnk1 \sim rbnk5$ の大小関係は、ステップS124で示した通り、 $rbnk1 < rbnk2 < rbnk3 < rbnk4 < rbnk5$ であるから、

5000円の電子小切手の振出許可通知文+ $rbnk2 + MACbnk2 + rbnk3 + MACbnk3 + rbnk5 + MACbnk5 + rbnk1 + MACbnk1 + rbnk4 + MACbnk4$

と並べ変える。

【0127】今、ICカード47から送信されてきた乱数は、 $rg4 < rg1 < rg2 < rg5 < rg3$ であるから、仮に、 $rb1=2$ 、 $rb2=3$ 、 $rb3=5$ 、 $rb4=1$ 、 $rb5=4$ とすると、サービス享受者11から受領した銀行15の乱数 $rbnk1 \sim rbnk5$ は、 $rbnk1 < rbnk2 < rbnk3 < rbnk4 < rbnk5$ である。よって、 $rbnk2$ 、 $rbnk3$ 、 $rbnk5$ 、 $rbnk1$ 、 $rbnk4$ の順に並べ変える。

【0128】次に、ステップS160において、ステップS159で並べ変えた電子小切手に、ステップS157で生成した $MACb$ と IDb とを加え、一方向性関数 $Facc$ とICカード47に記憶されている銀行15の公開鍵 $KPBNK$ とで暗号文 $Eacc$ を生成する。

【0129】 $Eacc = Facc(5000円の電子小切手の振出許可通知文 + rbnk2 + MACbnk2 +$

$MACbnk2' = H(5000円、振出銀行名、振出日時、\dots、rbnk2、KPBNK)$

$rbnk3 + MACbnk3 + rbnk5 + MACbnk5 + rbnk1 + MACbnk1 + rbnk4 + MACbnk4 + MACb + IDb, KPBNK)$

次に、ステップS161において、ICカード47は、銀行15に暗号文 $Eacc$ を送信する。ICカード47は、この暗号文 $Eacc$ が正常に銀行15に届いたことを確認すると、送信した電子小切手「5000円の電子小切手の振出許可通知文+ $rbnk1 + MACbnk1 + rbnk2 + MACbnk2 + \dots + rbnk5 + MACbnk5$ 」を無効化する。次に、ステップS162において、暗号文 $Eacc$ を受信した銀行15は、秘密鍵 $KSBNK$ により、この暗号文 $Eacc$ を下記のように復号化する。

【0130】5000円の電子小切手の振出許可通知文+ $rbnk2 + MACbnk2 + rbnk3 + MACbnk3 + rbnk5 + MACbnk5 + rbnk1 + MACbnk1 + rbnk4 + MACbnk4 + MACb + IDb = Facc * (Eacc, KSBNK)$

このようにして暗号文 $Eacc$ を復号化した銀行15は、ステップS163において、復号化したデータの IDb からICカード47の公開鍵 KPB を検索し、ステップS157で生成した乱数 $rg1 \sim rg5$ 、 IDb 等から下記のようにICカード47の署名を確認する。

【0131】 $MACb' = G(rg1, rg2, rg3, rg4, rg5, IDb, \dots, KPB)$

この $MACb'$ と、ステップS162で得られた $MACb$ とを比較し、同一であればICカード47の署名がされたものであると判断する。

【0132】次に、ステップS164において、ステップS157でICカード47に送信した乱数 $rg1 \sim rg5$ の大小関係からステップS162で暗号文 $Eacc$ を復号化した際に得られた $rbnk1 \sim rbnk5$ の大小関係の並びが正しいことを確認する。この例では、送信した $rg1 \sim rg5$ の大小関係が $rg4 < rg1 < rg2 < rg5 < rg3$ であったため、 $rbnk1 \sim rbnk5$ が $rbnk2$ 、 $rbnk3$ 、 $rbnk5$ 、 $rbnk1$ 、 $rbnk4$ の順序で並んでいることを確認する。もし、ここで乱数 $rbnk1 \sim rbnk5$ の並び順がステップS157でICカード47に送信した順序と異なる順番で受信した場合、銀行15が正当に発行したICカード47の中から送信されたものではなく、不正使用された電子小切手として銀行15は、以降の決済手順を停止する。

【0133】更に、ステップS165において、銀行15は、自身の公開鍵 $KPBNK$ を使用して下記のように $MACbnk1 \sim 5$ の署名を確認し、確かに自分自身によって振り出されたものであることを確認する。

【0134】

MACbnk3`=H(5000円、振出銀行名、振出日時、…、rbnk3

KPBNK)

MACbnk4`=H(5000円、振出銀行名、振出日時、…、rbnk4
、KPBNK)

次に、ステップS166において、銀行15は、自身が振り出した小切手であることが確認できれば、ステップS126で入金した自らの払出小切手支払に当てる口座21からサービス提供者27の口座35に5000円を振替え、その旨をICカード47に通知する。そして、次のステップS167において、ICカード47は、銀行15からの通知内容をサービス提供者27に通知する。

【0135】上述した実施形態では、説明を単純化するために図2の簡単化した電子小切手システムを例に取ったが、サービス提供者27はサービス享受者11から受領した電子小切手を図10及び図11に示した手順を実行することで、銀行15が発行したICカード(図示しない)を有する別の第三者(図示しない)に対しても支払うことができる。また、サービス提供者27が複数種類の金種の電子小切手を有する場合に、サービス享受者11から支払われた電子小切手に対して、ステップS147～S157で示した手順を逆方向に実行することでサービス提供者11はサービス享受者27に対しておつりを支払うこともできる。なお、この実施形態では、Fchr、Fpay、faccについては、RSA暗号方式のような安全性が確認されている公開鍵暗号方式を使用する方式としたが、暗号化に使用する鍵を一定期間毎(又はトランザクション毎)に変更するのであれば、DESやFEAL等の共通鍵暗号方式を用いることもできる。

【0136】また、署名を行う際に使用する関数(署名を確認する際に使用する関数)D*、H*、G*は、特開昭60-26378号公報(デジタル署名方式)等に開示されている方法で署名を行うことができる。

【0137】また、この実施形態においては、正規に銀行15が発行したICカード45、47であることの確認として、これらICカードのIDと公開鍵とに対して、銀行15の署名により、その正当性を確認したが、システムに共通の秘密情報を夫々のICカードが有することをゼロ知識証明法等で確認することでも可能である。

【0138】以上、この実施形態で示したように、銀行15が発行した電子小切手のデータは、他人に支払う時点でのデータの順序の並び変えが発生するが、データそのものを加工する訳ではないので、受領した側も振出人の署名を確実に確認できる。また、受取側も第三者に対

して受領した電子小切手で支払を行うことができる。

【0139】また、銀行を振出人とする電子小切手とすることで、その署名を確認するための公開鍵は、電子小切手の受取人共通となるため、鍵の管理が非常に容易となる。更には、銀行の公開鍵は、ICカード発行時に記憶させておけば、銀行の署名確認時、銀行や第三者の信用機関へ問い合わせる必要がない。

【0140】なお、上述した内容は、あくまで本発明の一実施形態に関するものであって、本発明が上記内容のみに限定されることを意味するものでないのは勿論である。

【図面の簡単な説明】

【図1】従来の電子小切手システムを示すブロック図。

【図2】本発明の一実施形態に係る電子小切手システムを示すブロック図。

【図3】一実施形態に係る電子小切手システムの構成要素を示す拡大図。

【図4】銀行からサービス享受者のICカード15に送信される暗号化データを示した説明図。

【図5】システム利用に際して必要な電子小切手帳の発行手順を示すフローチャート。

【図6】サービス享受者の銀行に対する電子小切手の振出依頼の手順を示すフローチャート。

【図7】サービス享受者の銀行に対する電子小切手の振出依頼の手順を示すフローチャート。

【図8】銀行に送信する通信文に付加する認証子を求めるための処理手順を示すブロック図。

【図9】銀行に送信する通信文を暗号化する場合の処理手順を示すブロック図。

【図10】サービス提供者に対する電子小切手での支払手順を示すフローチャート。

【図11】サービス提供者に対する電子小切手での支払手順を示すフローチャート。

【図12】サービス提供者と銀行間での電子小切手による決済手順を示すフローチャート。

【図13】サービス提供者と銀行間での電子小切手による決済手順を示すフローチャート。

【符号の説明】

11 サービス享受者

15 銀行

17 サービス享受者の銀行口座

21 銀行15の払出小切手支払口座

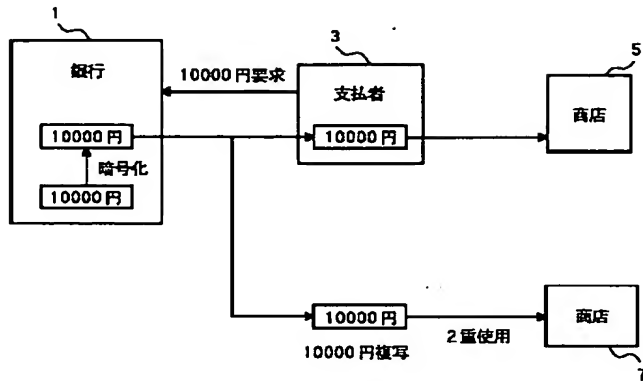
27 サービス提供者

41、43 端末機

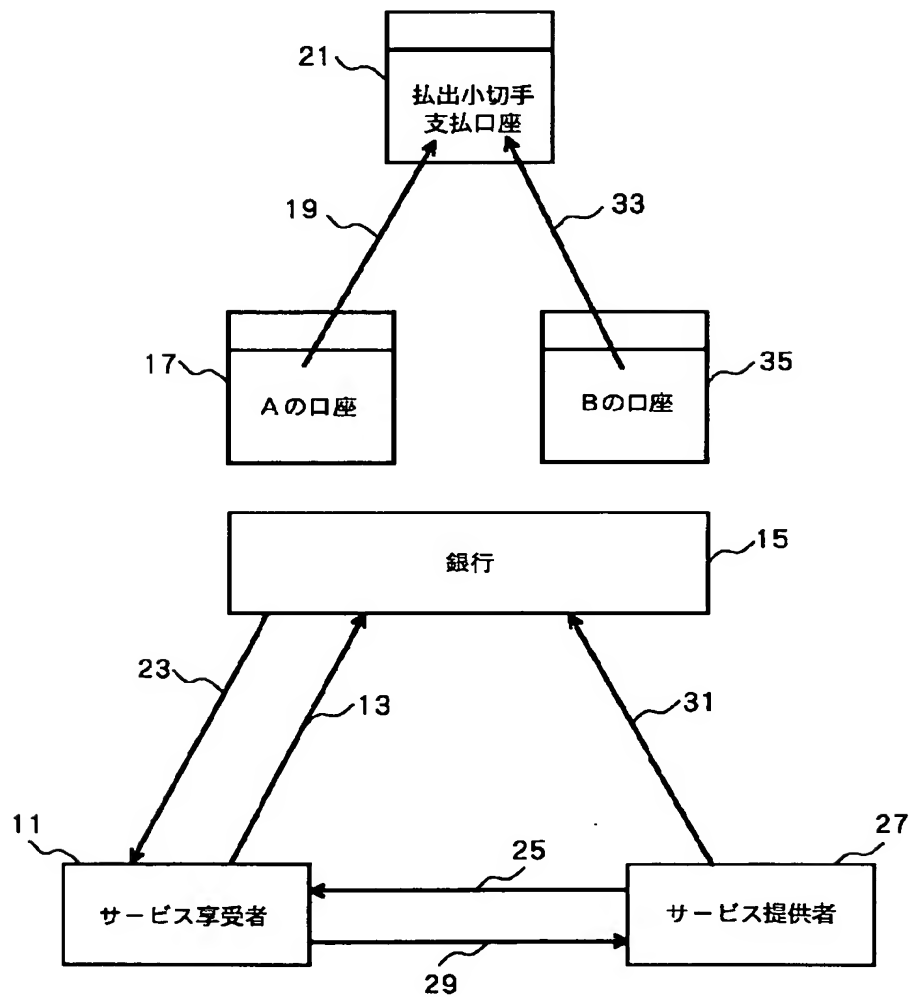
35 サービス提供者の銀行口座

45、47 ICカード

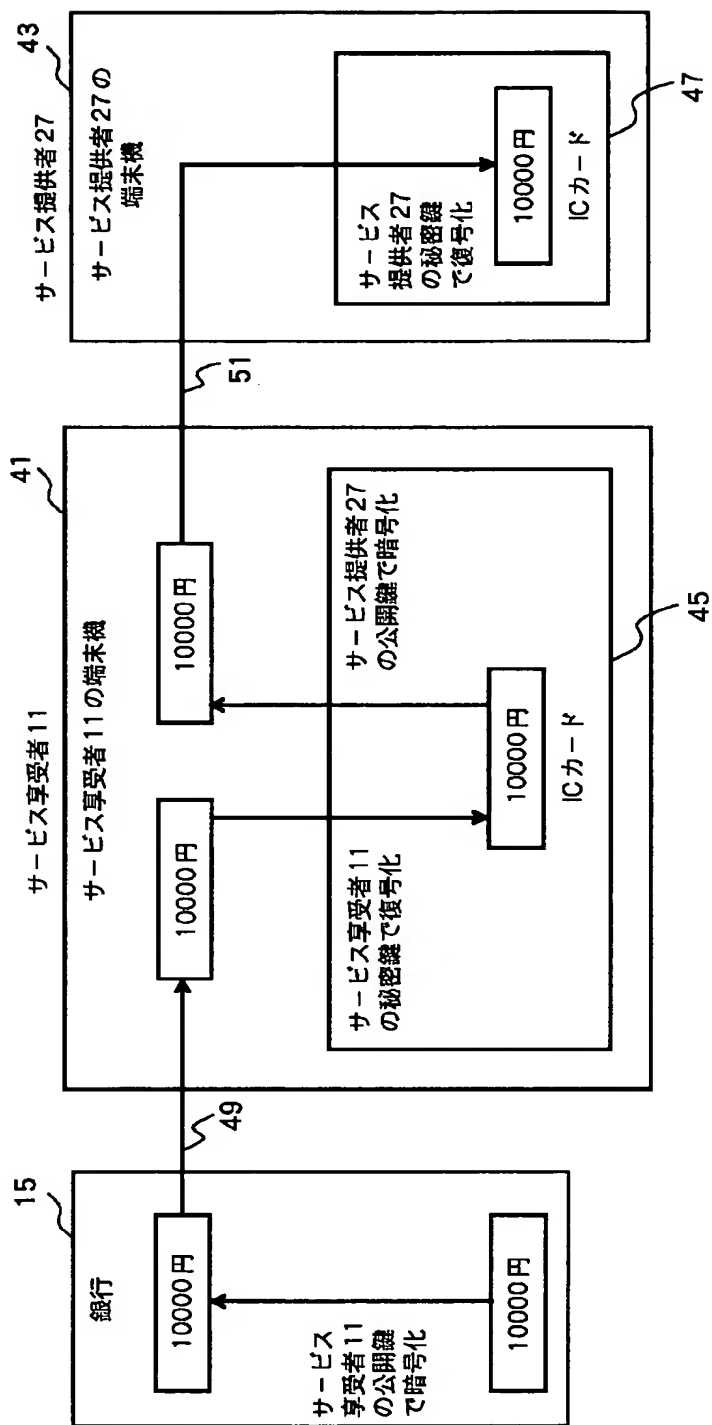
【図1】



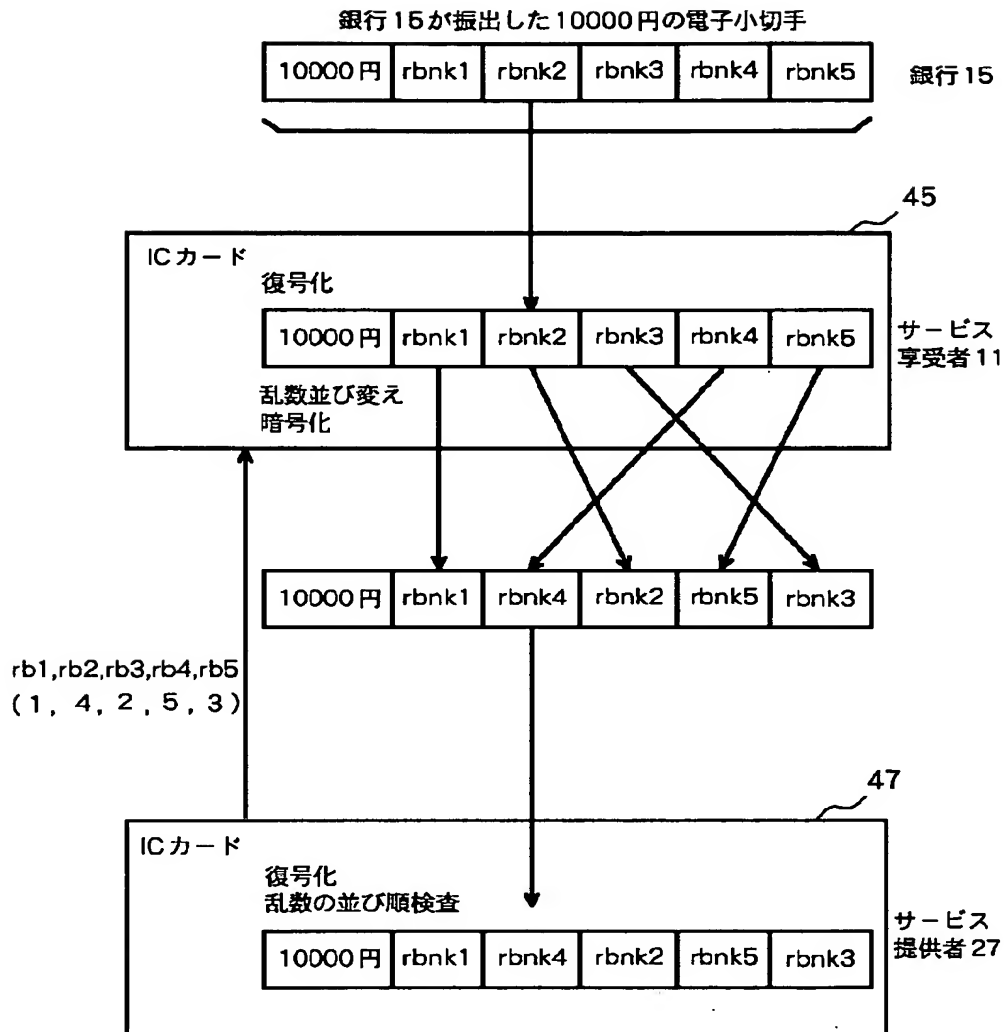
【図2】



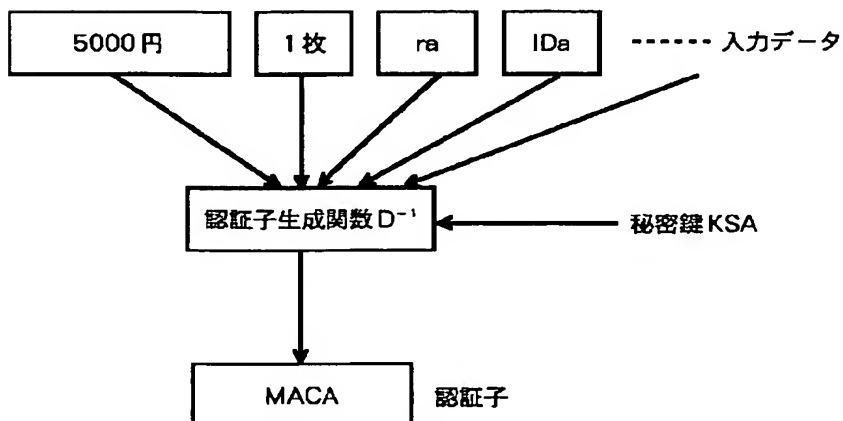
【図3】



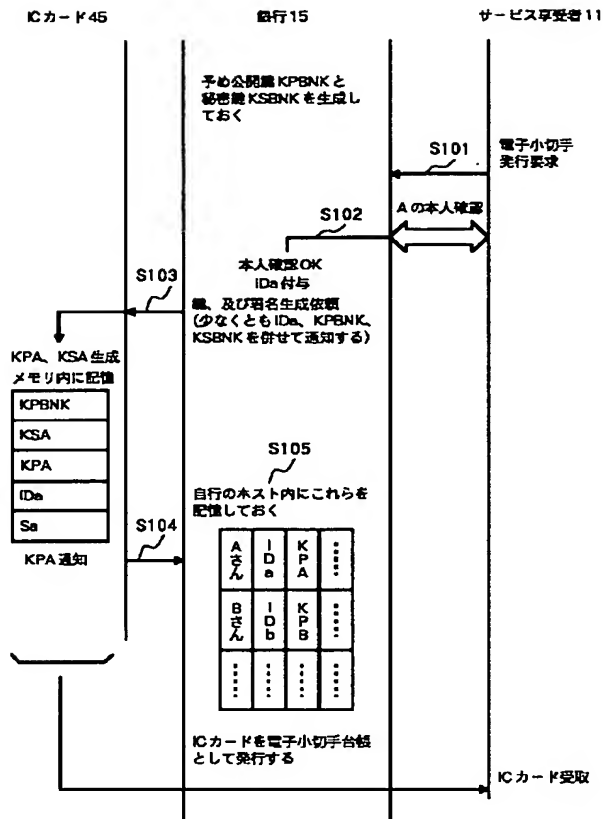
【図4】



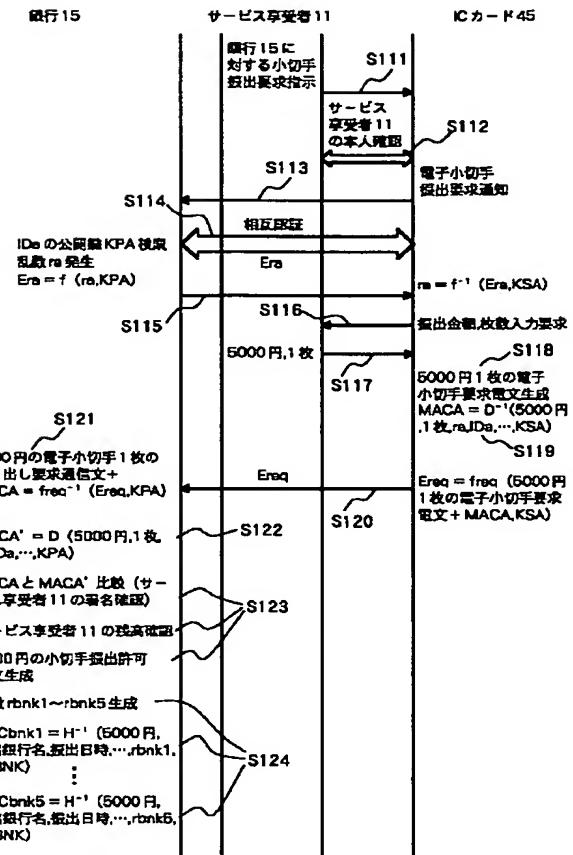
【図8】



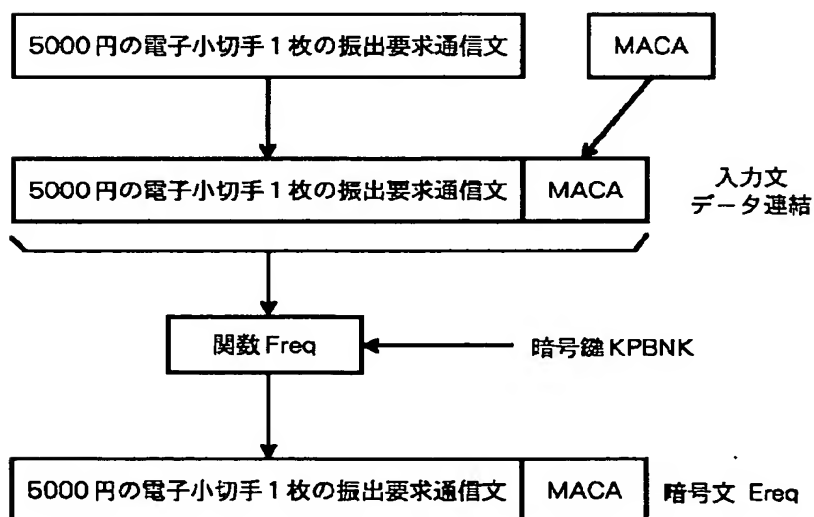
【図5】



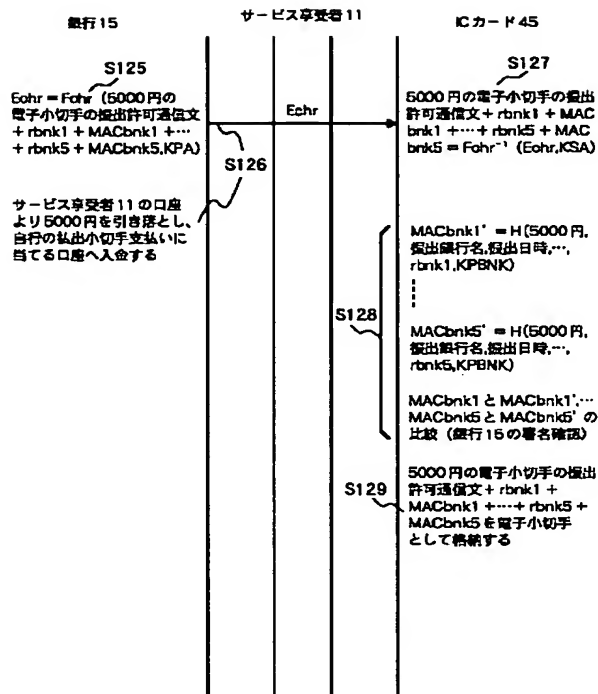
【図6】



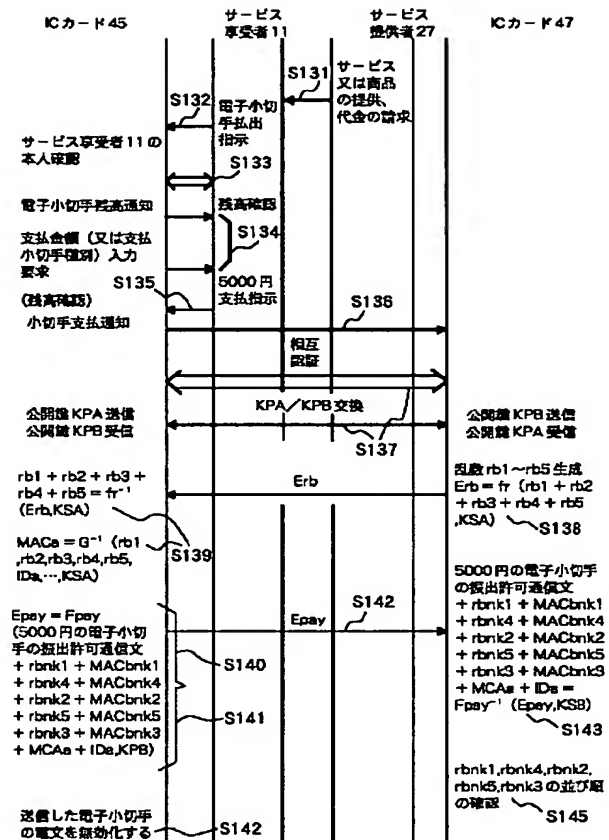
【図9】



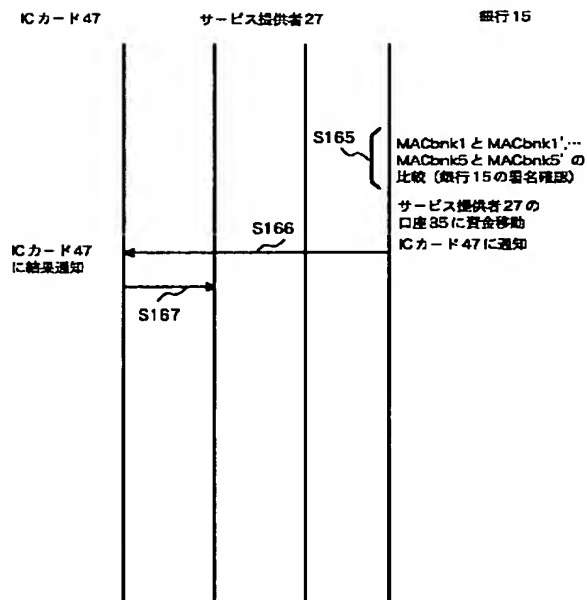
【図7】



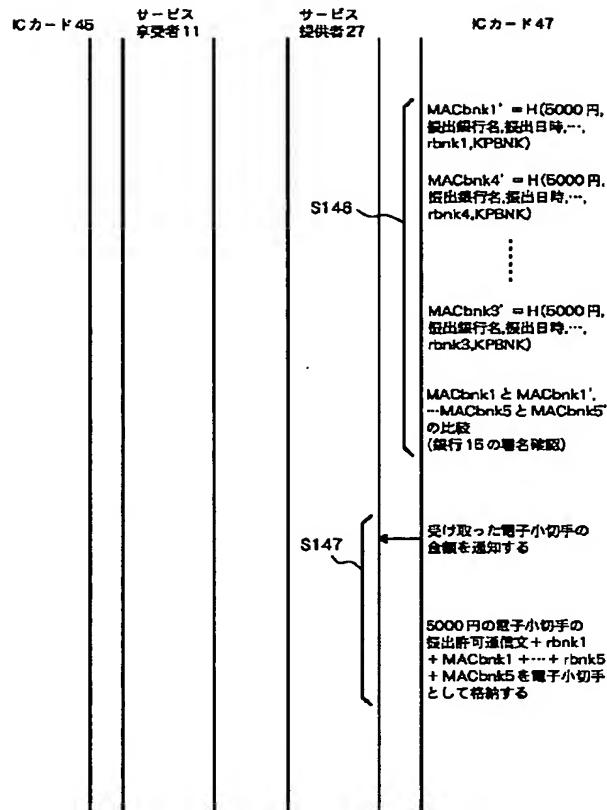
【図10】



【図13】



【図11】



【図12】

